Regulation Cell
5th Floor, Bharat Sanchar Bhawan,
Janpath,New Delhi – 110001
Tel.:011-2373 9295, Fax: 2373 4081
Email : agmregln@gmail.com

भारत संचार निगम लिमिटेड
(भारत सरकार का उपक्रम)

BHARAT SANCHAR NIGAM LIMITED
(A Govt. of India Enterprise)

To,

Advisor (QoS)
Telecom Regulatory Authority of India
Mahanagar Door Sanchar Bhawan
Jawahar Lal Nehru Marg, (Minto Road)
New Delhi-110002

{Kind attention: Sh. A. Robert J. Ravi, Advisor (QoS)}

No: Regln/1-44/2016/ dated: -07-2016

Sir,
Sub:- Comments of BSNL on TRAI's Consultation Paper on "Cloud Computing"

Kindly refer to the Consultation Paper on "Cloud Computing" dated 10-06-2016.
In this regard the BSNL's comments are as follows:-

Question 1. What are the paradigms of cost benefit analysis especially in terms of: a. accelerating the design and roll out of services b. Promotion of social networking, participative governance and e-commerce? c. Expansion of new services. d. Any other items or technologies. Please support your views with relevant data.

BSNL's Comment:

A cloud platform is more of a consumptive service, it saves organizations from the hassles of procurement delays, delayed times to roll out new services because of lack of scalable infrastructure, rather it gives businesses and the organizations to create an agile IT framework of launching new services, reduces time to market to evaluate new opportunities without large upfront CAPEX investments, it helps in consumerization of the online customer experience. The paradigms are:

1. Cost Optimization

    a) Reduced CapEX
    b) Lower Hardware & Power
    c) Pay-per-use
    d) On-Demand Elasticity
    e) Efficiency
    f) Economies-of-scale

2. Risk Optimization

    a) Business Continuity

b) Technology independence
c) Reduced Operational Complexity
d) Governance/Compliance
e) Data Sovereignty
f) Standardized Services

3. Strategic Agility

a) Time-to-market
b) Adaptive Systems
c) Rapid Development
d) New Business Models
e) Flexibility/Scalability
f) Resource Leverage

Question 2. Please indicate with details how the economies of scale in the cloud will help cost reduction in the IT budget of an organization?
BSNL's Comment:
• Economies of scale refers to the Cost Advantages that an enterprise obtains due to expansion. In economic terms, typically, a company that achieves economies of scale lowers the average cost per unit through increased production since fixed costs are shared over an increased number of goods. Bringing in the core IT infrastructure into large data centers with the Cloud can deliver advantage of economies of scale in three key areas:

1. Supply-side savings: Large-scale data centers (DCs) lower costs per server. For e.g. large-scale DCs can get more discounts on the purchases of hardware for and are likely to benefit more in comparison to the smaller DCs which are run inside enterprises, PUE is also lower in large data center, lowers labour cost by automating many repetitive task. Supply side economies of scale emanate from the following areas:

a) Cost of Power
b) Infrastructure Labour cost
c) Security & Reliability
d) Buying Power

2. Demand-side aggregation: The overall cost of IT is determined by the degree to which the capacity is efficiently utilized and not by the cost of capacity. With the concept of "virtualization", fewer servers are needed to carry the same number of workloads as multiple applications can run on a single physical servers. Moreover, workloads are highly variable over time. Aggregating demand for computing smoothest overall variability, allowing server

utilization rates to increase. For e.g. People checking email at different times, consumer services peaking in the evening & workplace services peaking the workday.

• Cloud helps an organization with the following business benefits:
1) It helps in lowering the opportunity cost of running technology.
2) It helps in allowing a shift from capital expenses to operating expenses.
3) It helps in lowering the total cost of ownership (TCO) of the technology by -
a) by giving transparent pricing based on different usage metrics - RAM, storage, bandwidth etc.
b) Savings over direct costs that accompany running a server like, power, floor space, storage and IT operations to manage these resources.
c) Savings over indirect costs as network and storage infrastructure and IT operations to manage the general infrastructure.
d) Savings over the overhead costs of owning a server as procurement and accounting personnel, IT management and its attention.

Question 3. What parameters do the business enterprises focus on while selecting type of cloud service deployment model? How does a decision on such parameters differ for large business setups and SMEs?
BSNL's Comment:
A business enterprise would primarily look at the following:
a) Performance - achieving high-speed delivery of applications.
b) Technology stack - depends on the nature of business that the organization is into and what are the key business drivers that are being fulfilled by various cloud deployment model like IaaS, PaaS or SaaS; whilst a big software house may consistently look for infra ready platform to do test and quality assurance of its applications thus leading to IaaS cloud, a SME/SMB enterprise might be more inclined towards a software ready cloud which is available for consumption leading to SaaS based cloud.
c) Service Level Agreements and Reliability - Whilst an enterprise client would be more concerned around hosting their key business applications on cloud unless the required SLAs are met, a small SMB client may not be too concerned around the same.
d) Security and Compliance - whilst these may be bigger barriers for adoption of cloud by large enterprises an SME / SMB are least bothered around compliance.

Question 4. How can a secure migration path may be prescribed so that migration and deployment from one cloud to another is facilitated without any glitches?
BSNL's Comment:
Currently all leading cloud service providers have their own pre-defined architecture and technology stack and there is no defined standard developed towards inter cloud migrations.

It requires a common set of APIs to be developed that can work across multiple cloud service provider platform.

Question 5. What regulatory provisions may be mandated so that a customer is able to have control over his data while moving it in and out of the cloud?
BSNL's Comment:
• For reference CAF of BSNL Cloud Services is attached.

Question 6. What regulatory framework and standards should be put in place for ensuring interoperability of cloud services at various levels of implementation viz. abstraction, programming and orchestration layer?
BSNL's Comment:
• ISO27001, CSA Cloud Control Matrix, standardized use of APIs like REST or SOA, data segregation, network abstraction are some of the key standards that needs to be put in place.

Question 7. What shall be the QoS parameters based on which the performance of different cloud service providers could be measured for different service models? The parameters essential and desirable and their respective benchmarks may be suggested.
BSNL's Comment:
For cloud service provider performance measurement can be based upon the following parameters:

  1) Elasticity
  2) Reliability
  3) Availability
  4) Latency between VMs
  5) Multi-tenancy and layer of abstraction
  6) Agility and adaptability
  7) Virtualization

Question 8. What provisions are required in order to facilitate billing and metering re-verification by the client of Cloud services? In case of any dispute, how is it proposed to be addressed/ resolved?
BSNL's Comment:
• Transparent metering and billing, which can be accessible by both Cloud Service Provider and customer can help to avoid disputes.

Question 9. What mechanism should be in place for handling customer complaints and grievances in Cloud services? Please comment with justification.
BSNL's Comment:

• In BSNL, every complaint is handled at Centralized Help desk where compliant handling & technical support assistance is provided.
• Suitable Escalation Matrix is also in place.

Question 10. Enumerate in detail with justification, the provisions that need to be put in place to ensure that the cloud services being offered are secure.
BSNL's Comment:
• For a secure cloud service offering, the provider must ensure the following:
• World class security architecture ensuring highest security levels.
• Five layers of security framework built over key security considerations.
A) Physical Security.
B) Infrastructure Security.
C) Audit & Compliance.
D) Customer Data Security.
E) Operational Security.
• ISO 27001 certified & SSAE 16 / ISAE 3402 compliant.

Question 11. What are the termination or exit provisions that need to be defined for ensuring security of data or information over cloud?
BSNL's Comment:
As per the agreement between Cloud Service Provider (CSP) and customer.
Question 12. What security provisions are needed for live migration to cloud and for migration from one cloud service provider to another?
BSNL's Comment:
Security provisions are different for different cloud deployment models and are as follows:
a) SaaS -
1) Data portability - SaaS vendor should provide a way to allow customers to control their application data; customers should have the ability to export data in a format that can be easily parsed and migrated to other internal and external applications
2) User Management - SaaS providers should enable a mechanism to import enterprise user information by supporting the use of Microsoft Active Directory or LDAP based services.
3) Security - Transparency in SaaS provider's security policies to be able to determine whether adequate security of data is provided.
b) PaaS -
1) Data Portability - In PaaS model, data is mostly stored in database, and should allow the customer to export the data in a format that can be migrated to other databases
2) User Management - Customers should ensure that PaaS providers user management aligns with their existing directory services and user management processes
3) Security - Customers should ensure that rogue applications hosted within the PaaS

platform should not be able to exploit vulnerabilities in the platform software to affect other applications. 4) Platform Management - PaaS deployment should allow customers to use similar tools to manage and tune customer applications

c) IaaS -

1) Data Portability - IaaS provider must provide a way to replicate or migrate the block or file data to a redundant system

2) Security - The IaaS provider should allow for RBAC profiles for server administrator, application administrator or database administrator

3) Auditing - Cloud service provider should allow independent auditing of security and compliance policies, using merging technologies

Question 13. What should be the roles and responsibilities in terms of security of (a) Cloud Service Provider (CSP); and (b) End users?

BSNL's Comment:

For cloud service provider the responsibilities include the following -

a) Data Centre Security

b) Infrastructure security

c) Network and platform security

d) Compliance and governance

e) Multi-tenancy and isolation

f) Management interface vulnerability addressing

g) Resiliency and availability

h) Handling of security incidents

i) Authentication & Authorization

For end users the responsibilities include the following -

a) Application hardening

b) Data Security & protection through use of encryption

c) Password management

d) Backup

e) Patch management & security fixes for application and OS

Question 14. The law of the user's country may restrict cross-border transfer/disclosure of certain information. How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation takes place? What disclosure guidelines need to be prescribed to avoid such incidents?

BSNL's Comment:

[a]   How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation takes place ?

      With cross border transfer or disclosure of information, businesses may find themselves in more disputes with counter parties before foreign courts or in the international arbitration,

where a party choses or the parties' contract requires. Litigation in foreign courts may be to obtain final judgment for money, damages.

2.Section 75 of the Information Technology Act 2000 as amended by the IT Amendment Act 2008:- Act to apply for offence or contraventions committed outside India (1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality. (2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

3. The provisions contained in Civil Procedure Code, Criminal Procedure Code are primarily dealing with offence committed in India; whereas, in the clouds, the data is spread across many jurisdictions including that on transit. Whereas, the provisions of Indian Penal Code extend its operation to extra-territorial offences committed by any citizen of India / any person in any place, committing an offence targeting a computer resource located in India.

4. Protection under Section 75 of the IT Act 2000 also extends to the offence or contravention committed outside India, involving a computer, computer system or computer network located in India. This also does not appear to offer a comprehensive solution, because, it is highly unlikely that the foreign courts will enforce the orders passed on the basis of this provision, even otherwise, provision is silent about computers located outside India. Criminal Procedure Code, on trial of offences categorically provide that part of the offence is to be committed in one local area i.e., India.

5. The Convention on Cybercrime also known as the Budapest Convention on Cybercrime or the Budapest Convention:- This is the first international treaty aiming to address Internet and Computer crime by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. The Convention defines Illegal Access, Illegal interception, Data Interference, System interference, Misuse of devices, Computer-related forgery, Computer related fraud, Offences related to child pornography and Offences related to copyright and neighboring rights.

6. It also sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data. In addition, the Convention contains a provision on a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Signatory Parties. It appears, India is not a signatory to the convention.

7. To effectively address the issue – where the cloud service provider moves data from jurisdiction to another, consequential amendments would require to be made to the appropriate laws revolving around the subject or to enact constitutional legal framework.

14 [b] what disclosure guidelines need to be prescribed to avoid such incidents?

1. Section 6A of the Information Technology Act 2000 as amended by the IT Amendment Act 2008, provides as follows:-

(1) The appropriate Government may, for the purposes of this Chapter and for efficient delivery of services to the public through electronic means authorize, by order, any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify, by notification in the Official Gazette.

Explanation: For the purposes of this section, service provider so authorized includes any individual, private agency, private company, partnership firm, sole proprietor form or any such other body or agency which has been granted permission by the appropriate Government to offer services through electronic means in accordance with the policy governing such service sector.

2. To avoid such incidents, besides the measures as stated at reply to Question 14(a), following are also suggested:-

2.1LICENSE / PERMIT WITH CONDITIONS:-   Pursuant to the enabling provisions of the Section 6A, while issuing such Licenses / Permits / Registration as the case be, to the Intermediaries, conditions/restrictions as deem fit may be attached thereto – mandating for granting of licenses/permits/registration only to the operators who have, or, agree to have their hosting centres / servers located within the geographical boundaries of India, as defined in the appropriate acts of the land; and operations shall be restricted to the Indian territory only.

2.2 Disclosure Guidelines:-There is no specific regulation pertaining to protection of data privacy of an individual, except the IT(Reasonable security practices and procedures and sensitive personal data or information) Rules 2011, issued by the MoC & IT, D/o IT, pursuant to the powers conferred by clause (ob) of sub-section (2) of Section 87 read with Section 43A of the IT Act.

2.2(i) Section 79 of the IT Act 2000 as amended by the IT Amendment Act 2008, provides exemption from liability to the Intermediary in certain cases. Accordingly, notwithstanding anything contained in any law for the time being in force, but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link hosted by him. In exercise of the powers conferred by clause (zg) of subsection (2) of section 87 read with sub-section (2) of section 79 of the Information Technology Act, 2000 (21 of 2000), the Central Government has already notified Information Technology (Intermediaries guidelines) Rules, 2011.

2.2(ii)Enforcement of these rules, under cloud segment appear difficult because, the data is fragmented and spread across many jurisdiction including those under transit, which are re-assembled for use.

2.3   Mandatory Signing of Agreements between the Intermediaries and Clients, with clear cut separate clauses is one suggested option:-

The parties concerned i.e., the Cloud Service Provider and the Client must mandatorily enter into agreements, which would categorically provide for storage of the data by the Cloud Service Providers in Computer Systems located within the geographical boundaries of India. For additional safeguard, different clauses with templates containing [a] Indemnification, [b] Protection of IPR, [c] Data Privacy; [d] Liability Clause etc., may also be inserted to help them understand the implications of breach by either party.

Question 15. What polices, systems and processes are required to be defined for information governance framework in Cloud, from lawful interception point of view and particularly if it is hosted in a different country?
BSNL's Comment:
Cloud hosting has to be mandatory to be in India only from security point of view.

Question 16. What shall be the scope of cloud computing services in law? What is your view on providing license or registration to Cloud service providers so as to subject them to the obligations thereunder? Please comment with justification.
BSNL's Comment:

[a]   What shall be scope of cloud computing services in Law ?

Cloud computing initially divided in three main segments [a] IaaS: Information as a Service; [b] PaaS: Platform as a Service; and [c] SaaS: Software as a Service. These segments are differentiated based on the types of services they provide.

New forms of cloud computing that are emerging to supplement these three basic segments e.g. UcaaS: Unified Communications as a service; AaaS: Anything as a Service.

In view of every likelihood of cross border transfer or disclosure of information in cloud computing, it is desirable that the law provides for cloud computing standards e.g. National Institute of Standards and Technology (NISIT) U.S.A. provided for U.S.Govt Cloud Computing Technology Roadmap.
 [b] What is your view on providing license or registration to Cloud Service providers so as to subject them to the obligations thereunder? Please comment with justification?

    Issue of Licenses/Permits/Registrations subject to Conditions:-From perusal of the provisions of the Information Technology Act 2000, it appears, the appropriate Government has powers to issue Permits/Licenses to the intermediaries.

2. While issuing such Licenses / Permits / Registration as the case be, to the Intermediaries, conditions/restrictions as deem fit may be attached thereto– mandating for granting of licenses/permits/registration.

3.Issue of Regulations:-Provisions of section 6A(1) clearly enables the Government to lay down standards/regulations requiring any service provider to set up, maintain and upgrade the computerized facilities and perform such other services.

Question 17. What should be the protocol for cloud service providers to submit to the territorial jurisdiction of India for the purpose of lawful access of information? What should be the effective guidelines for and actions against those CSPs that are identified to be in possession of information related to the commission of a breach of National security of India?

BSNL's Comment:
• On similar lines of other telecom service products such as landline, mobile etc

Question 18. What are the steps that can be taken by the government for: (a) promoting cloud computing in e-governance projects? (b) Promoting establishment of data centers in India. (c) Encouraging business and private organizations utilize cloud services (d) to boost Digital India and Smart Cities incentive using cloud.

BSNL's Comment:
• Build strong connectivity as the backbone e-Governance services for citizens.
• Build data content / repositories related to government services.
• Use of Open Source technology.
• Server consolidation and virtualization thus reducing server hardware per location by leveraging shared government infrastructure.
• Agile services delivery framework through the use of cloud computing from State Data Centers across the country. Other government controlled entities such as BSNL should be treated at par with State Data Centers.
• Secured ways of transactions for government services through the use of digital signatures.
• Interoperability of various state government systems for processing and sharing of information in a common format.
• Performance & Efficiency - to create a framework through scalable infrastructure where lakhs of access can be done easily without affecting performance.
• Integration of legacy systems and proprietary software - to allow for integration with legacy system with new systems developed and hosted on cloud.

Question 19. Should there be a dedicated cloud for government applications? To what extent should it support a multi-tenant environment and what should be the rules regulating such an environment?

BSNL's Comment:
A dedicated government cloud can help the following:
• To boost an agile services delivery framework towards e-governance projects.
• It would allow standardized approach to security assessment, authorization and continuous monitoring for cloud products and services.
• It would create a streamlined process for using mission critical applications and regulated IT workloads.
• It would help to meet the distinct needs of state and country's Union government agencies.
• BSNL Internet Data Centre may be utilized for this purpose along with NIC Data Centers.

Question 20. What infrastructure challenges does India face towards development and deployment of state data centers in India? What should be the protocol for information sharing between states and between state and central?

BSNL's Comment:

With respect to challenges India face towards development and deployment of data centers in India. There should be seamless information sharing protocols between states and state & center meeting all requisite security consideration.

Question 21. What tax subsidies should be proposed to incentivise the promotion of Cloud Services in India? Give your comments with justification. What are the other incentives that can be given to private sector for the creation of data centers and cloud services platforms in India?

BSNL's Comment:
Government should enable suitable tax subsidies for promoting cloud infrastructure so as to gain advantages from this technology.

This is for your kind information please

Encls: Reference CAF

Raghuvir Singh
AGM (Regln-II)